UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,646	03/16/2004	Harlan Seymour	20423-08590	3936

34415 7590 03/12/2009

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
LEWIS, ALICIA M	

ART UNIT	PAPER NUMBER
2164	

NOTIFICATION DATE	DELIVERY MODE
03/12/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/802,646
Filing Date: March 16, 2004
Appellant(s): SEYMOUR ET AL.

Jie Zhang (Reg. No. 60,242)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed December 5, 2008 appealing from the Office action mailed September 17, 2008

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2003/0101355	Mattsson	5-2003
US 2003/0167229 A1	Ludwig et al.	9-2003
US 2005/0097149 A1	Vaitzblit et al.	5-2005

Low et al. "DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions" ICEIS 2002 - Databases and Information Systems Integration, 2002, pp. 121-128

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1).

With respect to claim 1, Mattson teaches an apparatus for empirically adjusting access to a database, said apparatus comprising:

coupled to the database, a database discovery module configured to determine database structure and the user's authorized access to the database (paragraphs 32 and 34-36), the user's authorized access including a set of authorized database tables and authorized columns (paragraph 38);

coupled to the database, a command monitoring module configured to monitor the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns (paragraphs 33, 35 and 50) (*A preselected quantity can be any number of accesses, including just one access. Mattson teaches in paragraph 35 that a period of time can be defined as one single query, but can also be an accumulation of queries during a time period. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson*); and

coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare the user's actual accesses with the user's authorized accesses and configured to adjust the user's authorized accesses

taking into account results of the comparing by changing settings within a database access control module (paragraphs 37-39, 42-46 and 52).

Although Mattson teaches adjusting a user's authorized accesses to an authorized database table or an authorized column (paragraphs 38 and 46), he does not explicitly teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed.

Ludwig teaches a modular business transactions platform (see abstract), in which he teaches denying future access to authorized tables/columns that were previously authorized, but not accessed (paragraph 51) (*Ludwig teaches disabling a user's access after a certain number of days of nonuse. By disabling a user's access to the system, the user will be denied access to previously authorized database tables/columns, such as those handled by a host user in paragraph 44*).

It would have been obvious to a person having ordinary skill in that art at the time the invention was made to have modified Mattson by the teaching of Ludwig because denying future access to authorized tables/columns that were previously authorized, but not accessed would enable Mattson's intrusion detection system to be used in processing financial transactions and would provide more security measures to prevent intrusion, thus providing more functionality (Ludwig, paragraph 51).

With respect to claim 2, Mattson as modified teaches the apparatus of claim 1 further comprising, coupled to the database discovery module and to the analysis

module, a storage area configured to accumulate data generated by the command monitoring module (Mattson, paragraph 33).

With respect to claim 3, Mattson as modified teaches the apparatus of claim 1 wherein the command monitoring module is a sniffer (Mattson, paragraph 5).

With respect to claims 5 and 14, Mattson teaches:

discovering the user's authorized access to the database (paragraphs 32 and 34-36), the user's authorized access including a set of authorized database tables and authorized columns (paragraph 38);

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns (paragraphs 33 and 50) (*A preselected quantity can be any number of accesses, including just one access. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson)*;

comparing the user's actual accesses with the user's authorized access (paragraphs 37 and 42); and

adjusting the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server (paragraphs 37-39, 42-46 and 52).

Although Mattson teaches adjusting a user's authorized accesses to an authorized database table or an authorized column (paragraphs 38 and 46), he does not explicitly teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed.

Ludwig teaches a modular business transactions platform (see abstract), in which he teaches denying future access to authorized tables/columns that were previously authorized, but not accessed (paragraph 51) (*Ludwig teaches disabling a user's access after a certain number of days of nonuse. By disabling a user's access to the system, the user will be denied access to previously authorized database tables/columns, such as those handled by a host user in paragraph 44*).

It would have been obvious to a person having ordinary skill in that art at the time the invention was made to have modified Mattson by the teaching of Ludwig because denying future access to authorized tables/columns that were previously authorized, but not accessed would enable Mattson's intrusion detection system to be used in processing financial transactions and would provide more security measures to prevent intrusion, thus providing more functionality (Ludwig, paragraph 51).

With respect to claims 8 and 17, Mattson as modified teaches wherein the discovering step uncovers any:

tables of the database (Mattson, paragraphs 32 and 38);

columns of the database (Mattson, paragraph 32 and 38);

views of the database (Mattson, paragraph 32);

stored procedures of the database Mattson, (paragraph 53);

user-defined functions of the database (Mattson, paragraph 53); and

triggers of the database (Mattson, paragraph 53).

With respect to claims 9 and 18, Mattson as modified teaches wherein the adjusting step comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day (Mattson, paragraph 48);

automatically hardening the database selectively based on time of day;

alerting a database administrator (Mattson, paragraphs 43, 44 and 46); and

continuing to monitor the user's accesses to the database after conclusion of the observing step.

With respect to claims 11 and 20, Mattson as modified teaches wherein the database is automatically hardened using database specific application programming interfaces (Mattson, paragraphs 46 and 48).

With respect to claim 23, Mattson as modified teaches wherein the preselected quantity of actual accesses is sufficiently large that all expected functionalities of applications accessing the database are exercised (Mattson, paragraphs 28-29, 33 and 50) *(The only expected functionalities of applications appears to be users using clients*

to access information in the database. Therefore, any preselected quantity of access to the database by clients, is large enough that the expected functionality is exercised).

With respect to claim 24, Mattson as modified teaches storing data generated by the observing of the user's actual accesses to the database in a storage area (Mattson, paragraph 33).

With respect to claim 25, Mattson as modified teaches generating a map of which tables and columns of the database were accessed during the observing (Mattson, paragraphs 32 and 33).

With respect to claim 26, Mattson as modified teaches:

monitoring the user's actual accesses to the database during an extended period occurring after the preselected quantity of actual accessed have been observed (Mattson, paragraphs 35, 42 and 43) *(According to one embodiment, a preselected quantity may be the item access rate. When this is the case, an extended period may be considered any accesses that occur after the item access rate has been reached, as in paragraph 43);* and

generating an alert in real time regarding the user's actual accesses that are observed during the extended period that were not observed within the preselected quantity of the user's actual accesses (Mattson, paragraph 43) *(All accesses observed after the item access rate has been reached, are considered to be observed during the*

extended period, and not observed within the preselected quantity of accesses. When this is the case, as indicated in paragraph 43, an alert is generated.)

Claim 4, 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 above, and further in view of Low et al. ("DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions") ('Low').

With respect to claim 4, Mattson as modified teaches claim 1.

Mattson as modified does not teach wherein the database is a relational database accessed by a structured query language.

Low teaches a method for using fingerprints to detect illegitimate accesses to databases (see abstract) in which he teaches wherein the database is a relational database accessed by a structured query language (abstract).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Low because wherein the database is a relational database accessed by a structured query language would enable a fingerprinting process to be used to detect anomalous database accesses involving SQL statements (Low, column 1, page 122).

With respect to claims 10 and 19, Mattson as modified teaches wherein the database is automatically hardened using standard SQL commands (Low, abstract, page 126, column 1; Mattson, paragraphs 46 and 48).

Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 above, and further in view Vaitzblit et al. (US Patent Application Publication 2005/0097149 A1) (Vaitzblit').

With respect to claims 6 and 15, Mattson as modified teaches claims 5 and 14.

Mattson as modified does not teach further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

Vaitzblit teaches a data audit system (see abstract), in which he teaches further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database (paragraphs 11 and 48-51).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Vaitzblit because teach further comprising the step of generating at least one third party report based upon observing actual accesses to the database would enable an efficient data

audit system that would help organizations address data privacy and security issues (Vaitzblit, paragraph 7), and to additionally detect anomalies (Vaitzblit, paragraph 19).

(10) Response to Argument

A. Claims 1-6, 8-11, 14, 15, 17-20 and 23-26 – Mattson in view of Ludwig, Low, and Vaitzblit

Appellant argues that neither Mattson nor Ludwig teaches adjusting the user's authorized access taking into account results of the comparing step by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns. Examiner disagrees. Mattson teaches that an authorized user has access to specific database tables and/or columns (paragraph 38). He further teaches a third component adapted to compare access rates and inference patterns with stored accumulated results (paragraph 37). According to paragraphs 42-43, a user's access is monitored, compared to authorized item access rates, and analyzed to determine if the number of accesses exceeds an allowed access rate. If the number exceeds the authorized user's item access rate, the access control system is alerted. Further, if the item access rate is not exceeded, the user's access is also compared to any inference pattern included in the security policy (paragraph 44). If it determined that the combination of items accessed by the user matches the defined inference pattern, the access control system is alerted (paragraph 44). Upon generation of an alert (due to inappropriate database access as explained above), the

user's authorized access is altered (paragraph 46). Thus it is clear that Mattson teaches adjusting the user's authorized access (i.e. altering the user authorization) taking into account results of the comparing step (i.e. based on comparison of item access rates and inference patterns to a user's actual access) by changing settings within a database access control module (i.e. altering authorization in access control system).

The Examiner admitted that although Mattson teaches adjusting a user's authorized accesses to an authorized database table or an authorized column (paragraphs 38 and 46), he does not explicitly teach adjusting the user's authorization to deny future access to authorized tables/columns that were previously authorized, but not accessed. The Examiner relied on Ludwig to teach this limitation. Ludwig teaches the establishment of accounts, such as for host users, which may be used to handle database administration (paragraph 44). He further teaches disabling a user's account after a certain number of days on nonuse (paragraph 51). By disabling a user's account, the user will be denied the previous access he/she had, including access to previously authorized database tables/columns used to handle database administration. Thus, it is clear the Ludwig teaches adjusting the user's authorization to deny future access to authorized table/columns that were previously authorized, but not accessed (i.e. disabling an inactive account, such as that of a host user used for database administration). Therefore, Mattson in view of Ludwig teaches adjusting the user's authorized access taking into account results of the comparing step by changing settings within a database access control module to deny the user future database

access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns.

Appellant argues that Ludwig is not related to adjusting user access to databases. However, as explained above, Ludwig teaches the establishment of accounts, such as for host users, which may be used to handle database administration (paragraph 44), and further teaches disabling a user's account after a certain number of days on nonuse (paragraph 51). Thus, Ludwig is related to adjusting user access to databases.

Appellant further argues that if the combination denies the user future database access because of extended inactiveness, such inactiveness would not trigger the authorized access adjustment that takes into account the comparison result because authorized access adjustments in Mattson are triggered by query activities that are absent in extended inactiveness. Examiner disagrees. Appellant is attempting to argue the references individually. Mattson teaches that a user's authorization is altered in response to an alert (paragraph 46). In Mattson, the alerts are based on item access rate and inference pattern. However, when Mattson is combined with Ludwig, an alert may also be generated based on inactiveness. Thus, the combination of the references would teach adjusting/altering user authorization based on item access rate, inference patterns, or inactivity. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642

F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Appellant further argues that the combination of Mattson and Ludwig does not work because the claimed observed preselected quantity of actual accesses would have to be zero activity in order for Ludwig to be applicable. Examiner disagrees. The second limitation of claim 1 calls for monitoring the user's actual accesses until a preselected quantity of actual accesses have been observed. The third and last limitation of claim 1 calls for comparing the user's actual accesses with the user's authorized accesses to adjust the user's authorized access to deny future database access. However, there is no claim language that ties the second and third/last limitations together. In other words, the accesses observed by the command monitoring module in the second limitation do not have to be the same accesses compared by the analysis module in the third limitation of claim 1. The analysis module is not required to compare the actual accesses observed by the command monitoring module with the user's authorized access; the claim language does not recite this limitation. In fact, there is no claim language that requires the second limitation to occur before the last limitation; thus, the last limitation (comparing the user's actual access…to deny future database access) may occur before the second limitation, in which case the user's actual accesses is definitely not limited to a preselected quantity and could include any number of accesses. Thus the comparison done by the analysis module may include comparing any number of actual accesses, including zero, with the user's authorized access.

B. Claim 25 – Mattson in view of Ludwig

Appellant argues that Mattson in view of Ludwig does not teach claim 25 because the claim implicitly recites that some tables and columns were actually accessed during observation, and further because Ludwig does not expire the account if there are actual accesses. The Examiner disagrees. As argued above, the observing step, comparing step, and adjusting step of claim 5 are not required to happen in any particular order. Thus, comparing the user's actual accesses with the user's authorized access and adjusting the user's authorized database access taking into account the results of the comparing step may occur before the observing the user's actual access to the database until a preselected quantity of actual accesses have been observed. Therefore, the number of actual accesses that are compared to the user's authorized access is not limited to a preselected quantity and can be any number of accesses, including zero. The map generated in claim 25 relates to the tables/columns accessed during the observing step and not the table/column access compared to the user's authorized access during the comparing step; there is no claim language that ties to two steps together or requires one to happen before the other. Thus, Ludwig can in fact be combined with Mattson, and the combination teaches generating a map of table of which tables and columns were accessed during the observing.

C. Claim 26 – Mattson in view of Ludwig

Lastly, Appellant argues that Mattson does not teach generating an alert in real time regarding the user's actual accesses that are observed during the extended period

that were not observed within the preselected quantity of the user's actual accesses. Examiner disagrees. Mattson teaches that an item access rate is the maximum number of rows of a column that a given user may access during a given period of time. The period of time can be defined as one single query or an accumulation of queries during a period of time (paragraph 35). Thus, either a single query (i.e. a preselected quantity of one) or the accumulation of queries during a time period may define the preselected quantity of actual accesses. Mattson further teaches that if a number of rows accessed exceeds an item access rate, an alert is generated (paragraph 43). When the item access rate defines the preselected quantity of actual accesses, any rows accessed exceeding the number defined by the item access rate may be considered actual accesses observed during the extended period because the rows are accessed after the preselected quantity (item access rate) has been reached. Any rows accessed after the preselected quantity has been reached (i.e. exceeding an item access rate) are not observed within the preselected quantity of accesses. When this is the case, an alert is generated (paragraph 43). Thus Mattson teaches generating an alert in real time regarding the user's actual accesses that are observed during the extended period (i.e. after the item access rate is reached) that were not observed within the preselected quantity of the user's actual accesses (i.e. accesses observed exceeding an item access rate).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/A. M. L./
Examiner, Art Unit 2164
March 9, 2009

Conferees:

/James Trujillo/

Supervisory Patent Examiner, Art Unit 2169

/Charles Rones/

Supervisory Patent Examiner, Art Unit 2164